IVT Analysis

Executive Summary

Three applications were flagged at different hourly change-points. On the other hand, three apps remained below threshold (IVT > 0.5). Then, post-spike IVT settles near 1.0, not interpreted by idfa_ip_ratio≈1 or requests_per_idfa≈1.06–1.11, thus indicating more of a source/signature shift rather than IP crowding or rate surges.

Methods

Daily and hourly master tables were derived from cleaning the data of six sheets; First_high_IVT was detected per app from hourly >0.5 IVTs; per app mean pre and post was computed for IVT, idfa_ua_ratio, idfa_ip_ratio, requests_per_idfa, unique_idfas, and unique_uas; There have been created hourly IVT timelines and Valid vs Invalid distributions.

Flag Summary

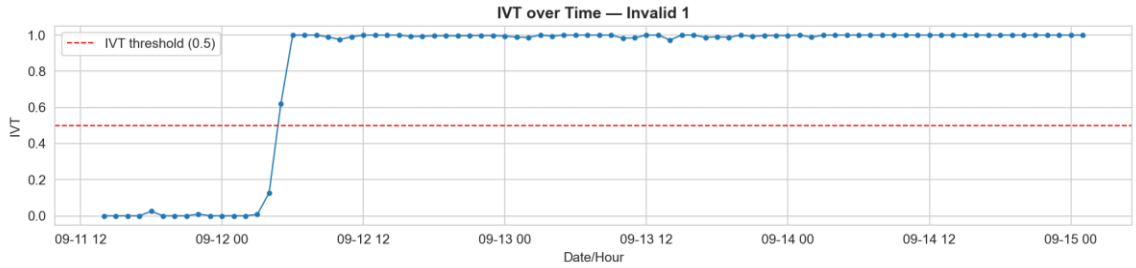
App ID	Status	First High IVT	Flag Type
Invalid 1	Invalid	2025-09-12 05:00:00	Delayed
Invalid 2	Invalid	2025-09-11 21:00:00	Early
Invalid 3	Invalid	2025-09-13 05:00:00	Delayed
Valid 1	Valid	N/A	Never flagged
Valid 2	Valid	N/A	Never flagged
Valid 3	Valid	N/A	Never flagged

Before/After Deltas

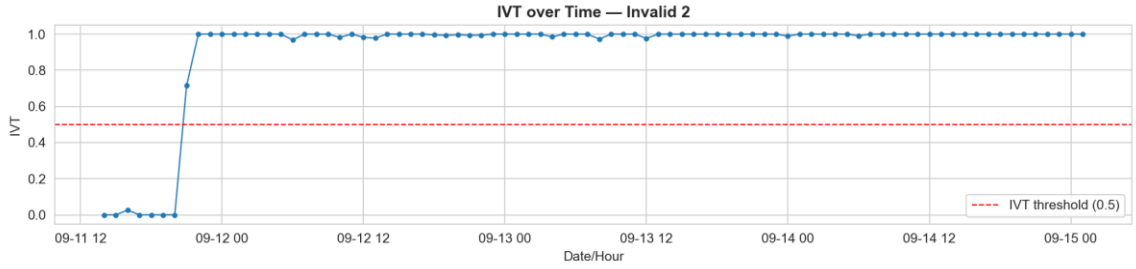
App ID	Metric	Before Mean	After Mean	Delta Ratio
Invalid 1	IVT	0.261	0.998	3.829
Invalid 1	idfa_ua_ratio	622.598	412.045	0.662
Invalid 1	requests_per_idfa	1.118	1.104	0.987
Invalid 1	unique_uas	215.333	220.833	1.026
Invalid 2	IVT	0.274	0.997	3.640
Invalid 2	idfa_ua_ratio	33.658	62.438	1.855
Invalid 2	requests_per_idfa	1.037	1.086	1.047
Invalid 2	unique_uas	774.000	875.375	1.131
Invalid 3	IVT	0.162	0.995	6.155
Invalid 3	idfa_ua_ratio	485.106	275.495	0.568
Invalid 3	requests_per_idfa	1.206	1.117	0.927
Invalid 3	unique_uas	198.800	197.250	0.992

Evidence Figures

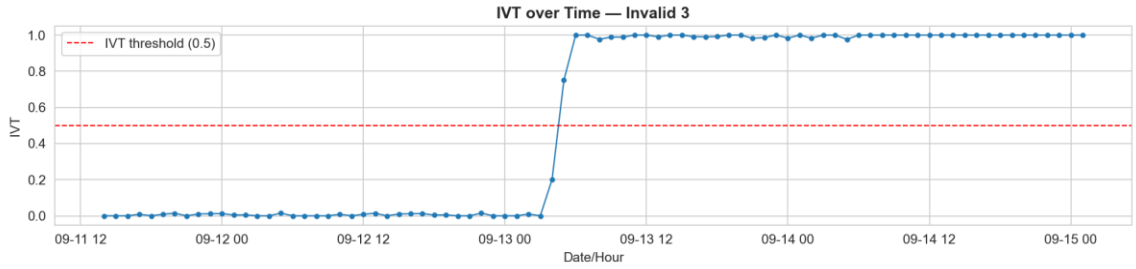
IVT timeline Invalid 1



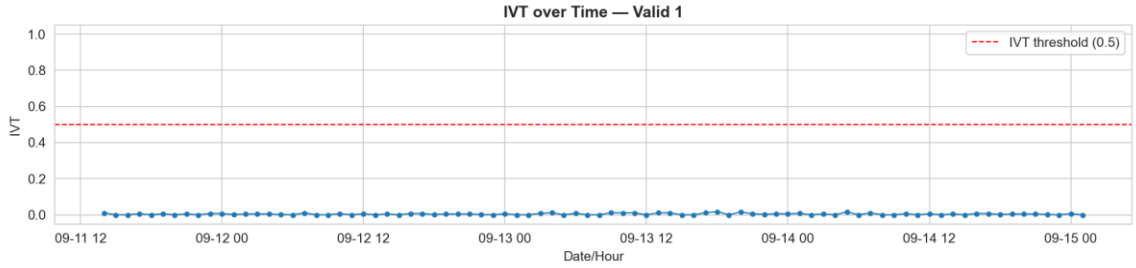
IVT timeline Invalid 2



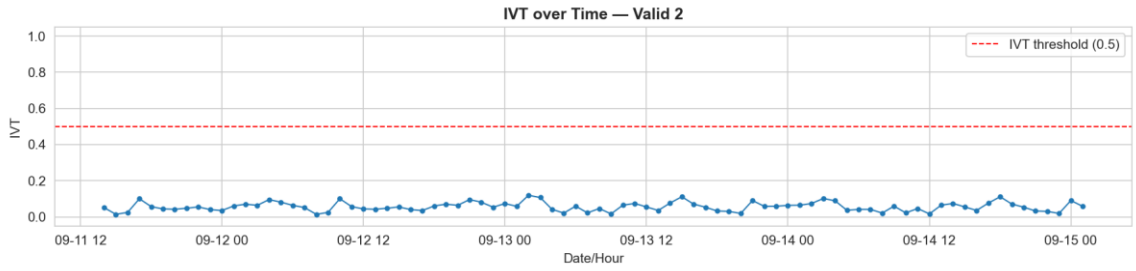
IVT timeline Invalid 3



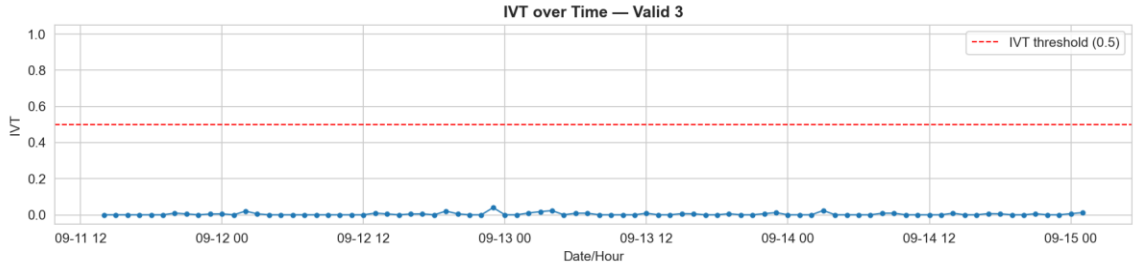
IVT timeline Valid 1



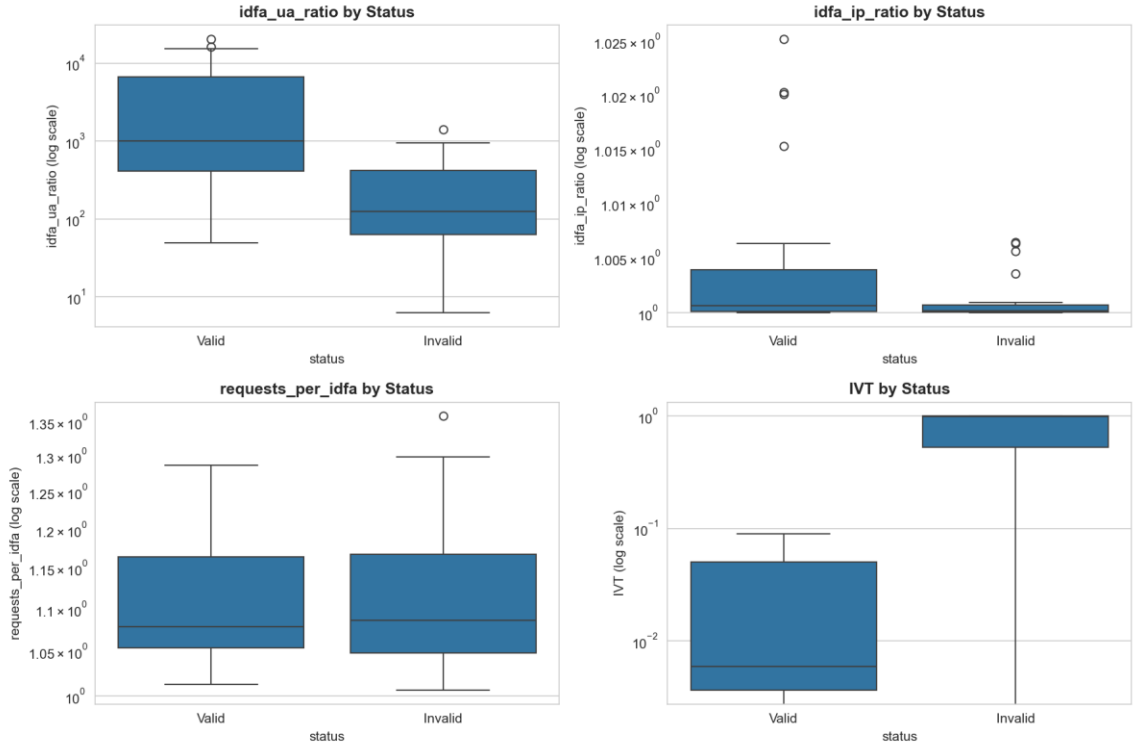
IVT timeline Valid 2



IVT timeline Valid 3



valid vs invalid boxplots



Interpretation Guide

- If IVT was immediately high, this indicated suspicious traffic by the app in the start; the evidence is that IVT>0.5 at first measurements and is sustained near-1.0 values.
- If IVT jumped later, we could conclude that a partner/campaign or SDK change has most likely introduced something suspicious at that hour; the evidence is in the detection of a step-change and persistent high IVT.
- If never flagged but with odd ratios, the situation may reflect benign UA homogeneity or signals not covered by this dataset; monitor further.

Recommendations

- Alerts should be triggered if hourly IVT crosses 0.5, and investigation should include a very detailed study of what the exact change-point hour was for partner/source toggles.
- If the spike arrives, throttle/block sources and add allow-lists for known good traffic to minimize false positives.
- Once raw IPs/UAs are available, the GeoIP/ASN enrichment and UA parsing should be added to link the spikes to either datacenters or synthetic UA clusters.

Appendix

The apps covered: Invalid 1, Invalid 2, Invalid 3, Valid 1, Valid 2, Valid 3.

Inputs: outputs/daily_master_clean.csv, outputs/hourly_master_clean.csv, outputs/summary_by_app.csv, outputs/first_high_IVT_per_app.csv, outputs/app_flag_summary.csv, outputs/before_after_deltas.csv; Figures from figures/.